ABSTRACT OF THE DISCLOSURE

The present invention provides a data processing apparatus and method for managing access to a memory within the data processing apparatus. The data processing apparatus comprises a processor operable in a plurality of modes and a plurality of domains, said plurality of domains comprising a secure domain and a non-secure domain, said plurality of modes including at least one non-secure mode being a mode in the non-secure domain and at least one secure mode being a mode in the secure domain, said processor being operable such that when executing a program in a secure mode said program has access to secure data which is not accessible when said processor is operating in a non-secure mode. Further, a memory is provided for storing data required by the processor, and consists of secure memory for storing secure data and non-secure memory for storing non-secure data. The memory further contains a non-secure table and a secure table, the non-secure table being within the non-secure memory and arranged to contain for each of a number of first memory regions an associated descriptor, and the secure table being within the secure memory and arranged to contain for each of a number of second memory regions an associated descriptor. When access to an item of data in the memory is required by the processor, the processor issues a memory access request, and a memory management unit is provided to perform one or more predetermined access control functions to control issuance of the memory access request to the memory. The memory management unit comprises an internal storage unit operable to store descriptors retrieved by the memory management unit from either the non-secure table or the secure table, and in accordance with the present invention the internal storage unit comprises a flag associated with each descriptor stored within the internal storage unit to identify whether that descriptor is from the non-secure table or the secure table. By this approach, when the processor is operating in a non-secure mode, the memory management unit is operable to perform the predetermined access control functions for the memory access request with reference to access control information derived from the descriptors in the internal storage unit retrieved from the non-secure table. In contrast, when the processor is operating in a secure mode, the memory management unit is operable to perform the predetermined access control functions for the memory access request with reference to access control information derived from the descriptors in the internal storage unit

retrieved from the secure table. This approach enables different descriptors to be used for the control of accesses to memory in either the secure domain or the non-secure domain, whilst enabling such different descriptors to co-exist within the memory management unit's internal storage unit, thereby avoiding the requirement to flush the contents of such an internal storage unit when the operation of the processor changes from the secure domain to the non-secure domain, or vice versa.

(Fig. 37)